IDC

May 2026
InfoBrief
Sponsored by

Lenovo | intel

Cyber-Resilience in Education

Ensuring Learning Never Stops



Shilpi Handa
Associate Director Research
Security and Trust, IDC



Table of contents



Click any title to navigate directly to that page.

In this InfoBrief 3

How education leaders see their own readiness 4

What the past two years did to classrooms and campuses 5

When the community becomes part of the attack surface 6

One device per student, one team for thousands 7

The gaps that remain hidden until an incident 8

Trusting the tools and vendors behind the classroom 9

From firefighting to foresight: What AI in security should deliver 10

Redefining “good enough” endpoint security 11

Why leaders still struggle to change the security model 12

A security model that fits education, not the other way around 13

About the IDC analyst 14

Message from the sponsor 15

In this InfoBrief

From managed to optimized — raising cybermaturity in education:



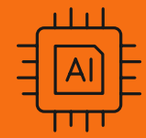
Most institutions sit in the "good but not great" zone. Security is structured and funded but is still too dependent on people, point tools, and legacy architectures to reliably prevent disruption. The real need now is to translate existing spend into smoother operations, fewer crises, and a more automated, optimized security posture that reduces day-to-day complexity for lean teams.

Breach costs and downtime — the business case for resilient endpoints:



Incidents are no longer edge cases but a recurring part of campus life, spanning phishing, data leaks, insider misuse, supply chain exposure, and attacks that reach below the OS. When they land, they disrupt teaching and research for days or weeks and strain already stretched teams and can force painful trade-offs across IT priorities — making resilience and faster recovery a strategic necessity, not just a technical upgrade.

Securing the hybrid, AI-enabled campus — devices, BYOD, supply chain, and AI:



Campuses now run on a mix of institution-owned and personal devices, cloud services, and AI-driven tools, all stitched together by inconsistent endpoint controls and visibility gaps. Leaders increasingly want embedded, hardware-level security and simpler, more unified management so they can apply consistent policies across this hybrid landscape, reduce blind spots, and trust the devices and vendors they depend on.

How education leaders see their own readiness

Digital infrastructure is now the backbone of education. Tools like learning management systems (LMSs), student information systems (SISs), and AI-enabled platforms are now the default, but this rapid shift has expanded the attack surface faster than cybersecurity maturity, leaving many leaders admitting they are still not ahead of increasingly sophisticated threats.

Key finding: Cybersecurity maturity level of the education sector

40%
of institutions classify their cybersecurity programs as "managed" (measured, monitored, and regularly reviewed).

23%
of institutions classify themselves as "optimized" (proactive and predictive).

4%
of institutions still operate in an "ad hoc" manner.

The baseline structures are largely established, but most institutions are yet to transition to a forward-looking security posture.

Key finding: Average budget spend and team size

- The average cybersecurity share of the overall IT budget is approximately 11–12%, and the cybersecurity team has approximately 11–12 dedicated security FTEs per institution.

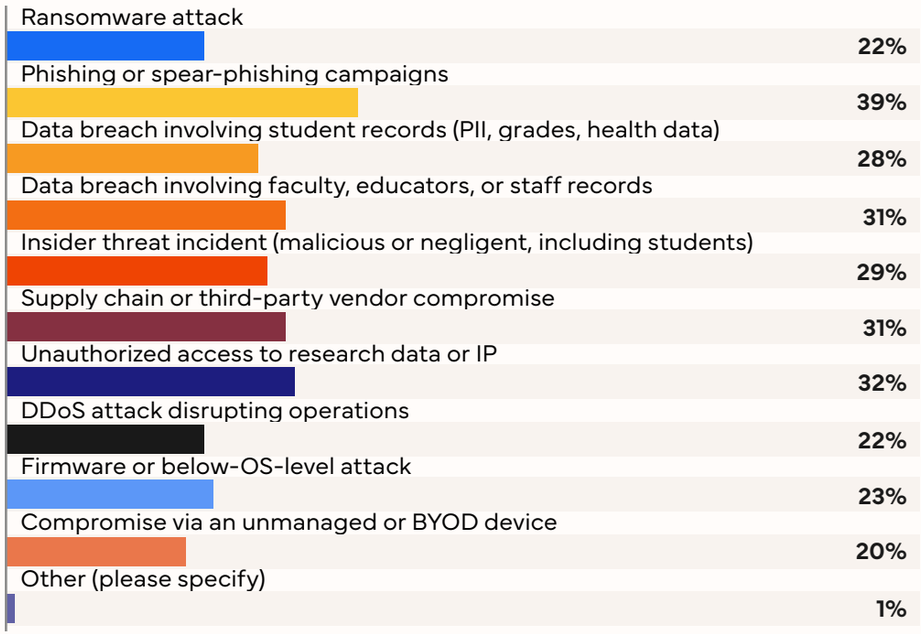
Despite decent spend and sizable teams, many institutions still feel "not yet optimized." The problem is less about budget and more about **how** resources are used: Fragmented tools, ineffective automation, and poor integration keep security investments from turning into real, measurable resilience.



What the past two years did to classrooms and campuses

Perhaps it's not just efficiency, but the sector's unique risk profile that prevents education from reaching "optimized" security. The IDC survey reveals a strikingly broad mix of incidents over the past two years, spanning every stage of the student and institutional data lifecycle. In addition, nearly 32% of respondents identified protecting faculty, educator, and staff data as a top security expectation.

Q. Has your institution experienced any of the following cybersecurity incidents in the past two years? (Select all that apply.)



IDC's *Lenovo Security Education Sector Survey*, April 2026 (n = 137)

Key findings: Financial impact of threats

- The most severe incident typically causes around **10 days** of disruption, pushing many institutions into multiday or even multiweek operational impact.
- The average financial hit is roughly **$880,000/ incident**, pulled up toward the million-dollar mark by a meaningful tail of breaches above $1 million, meaning a single major event can consume a large slice of an annual IT or security budget.

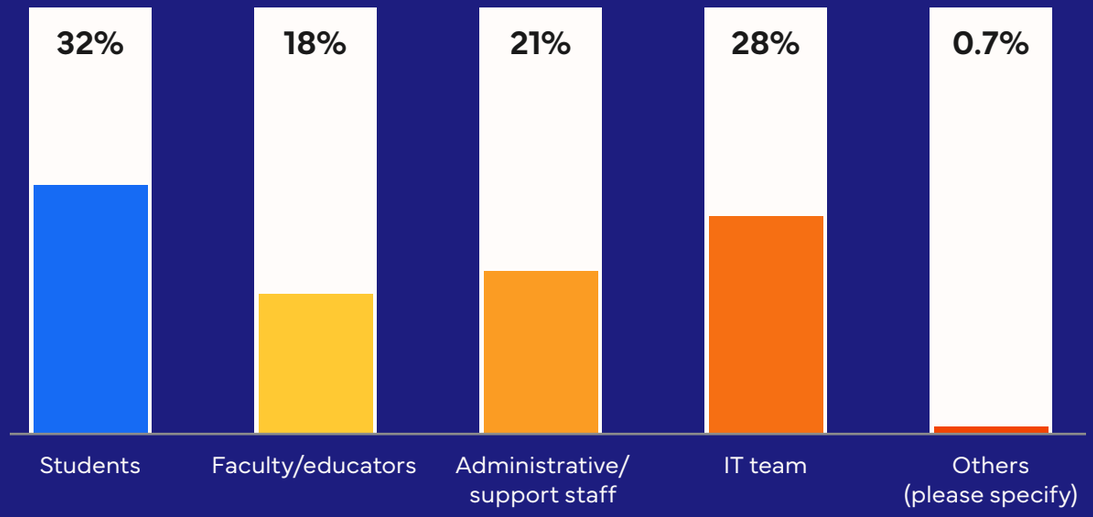


Cyberincidents in education are no longer low impact or opportunistic; they are **operationally disruptive and financially consequential.**

When the community becomes part of the attack surface

The research highlights that the human fabric of campuses' students, faculty, staff, and IT teams themselves is now a key part of the attack surface. In some markets, such as New Zealand, concern about students is overwhelming, while in others, such as India, faculty are perceived as the primary underestimated risk.

Q. In your opinion, which of the following groups represents the most significant and underestimated cybersecurity risk to your institution?



IDC's *Lenovo Security Education Sector Survey*, April 2026 (n = 137)



About **64%** of institutions say attack sophistication has risen in the past two years, underscoring how a distributed, nonexpert user base and overloaded IT teams are outgrowing manual controls and pushing the need for automation, behavior-based detection, and self-healing endpoints.

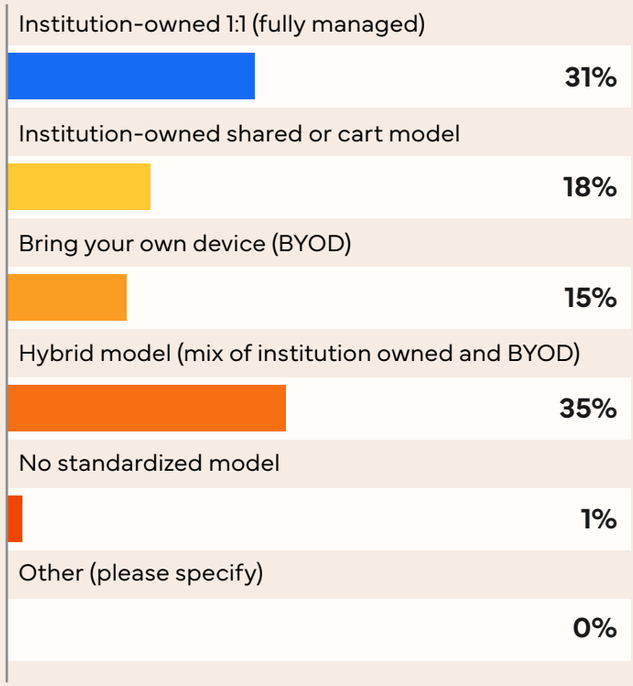
The risk of PII-related attacks is a major concern for 48% of institutions, driven by the significant consequences of a breach, including regulatory exposure, reputational damage, loss of student and staff trust, and increased risk of fraud and identity theft.



One device per student, one team for thousands

Endpoint estates in education are huge relative to team size: Each institution manages roughly 7,000 endpoints, effectively operating at large enterprise scale. At the same time, device models are highly diverse and heavily hybrid; 35% of respondents use a hybrid model, so some endpoints are tightly managed, while others are loosely governed — raising patching and configuration drift risk and increasing data leakage via unmanaged apps and exposure on insecure networks or from lost/stolen devices. Higher education also has to juggle FERPA, GDPR, HIPAA, NIST, and sector frameworks at once, making consistent endpoint, data, and supply chain controls even more critical than in single-regime industries.

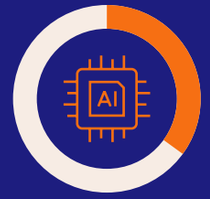
Q. What is your primary device deployment model for students?



The risk profile of education doesn't yet match its toolset. Even as attacks diversify, endpoint security is still dominated by legacy controls:



38% of institutions use traditional AV



Only **35%** of institutions use EPP, EDR, or AI-powered behavioral detection

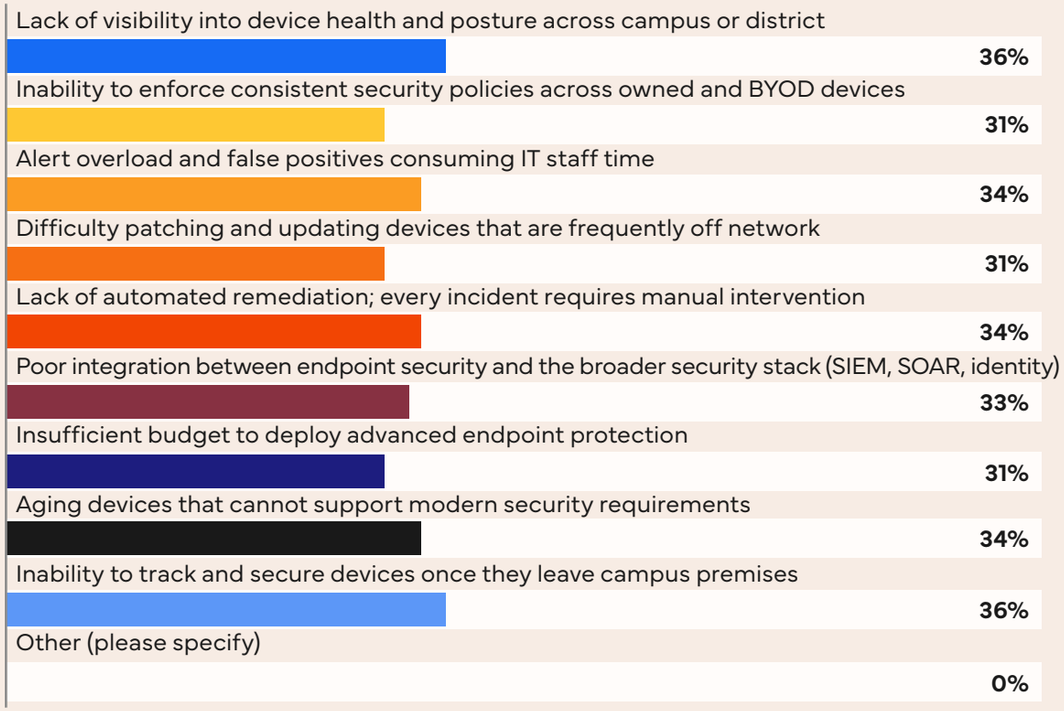
This means fewer than half of institutions have moved to truly modern, AI-driven, and self-healing protection — leaving a complex threat landscape defended by a largely traditional stack.

IDC's *Lenovo Security Education Sector Survey*, April 2026 (n = 137)

The gaps that remain hidden until an incident

Pain point data reinforces these perceived gaps

Q. (Overall) What are the top 3 pain points in managing endpoint security across your institution?



When education leaders rate controls by layer, a clear hierarchy appears:

- OS, application, and encryption controls are strongest, with roughly **76–78%** of institutions saying these are well or fully addressed.
- Hardware integrity and automated patching are close behind, at about **70%**.
- In contrast, **firmware/BIOS security, supply chain integrity, AI/ML behavioral detection, self-healing**, and **even device-level IAM all sit notably lower,** at less than 50%.

The riskiest layers of the security stack remain the least protected, even though they matter most in fleet-heavy, hybrid device, multivendor environments and during sophisticated ransomware or supply chain–driven attacks.



Taken together, the gaps point to a different model: AI-powered XDR, behavior-based analytics, and self-healing, automated recovery built into the endpoint itself — not just another bolt-on security layer sitting on top.

IDC's *Lenovo Security Education Sector Survey*, April 2026 (n = 137)

Trusting the tools and vendors behind the classroom

Third-party endpoints and education apps on student and staff devices uniquely amplify software supply chain risk for the education sector, making third-party dependence a distinct and growing point of anxiety for the sector's technology leaders.

Among the institutions surveyed:



57%
are most alarmed by pre-installed malware or compromised firmware on new devices



55%
worry about counterfeit or tampered hardware components embedded in devices.



43%
highlight breaches at third-party edtech vendors exposing student data.



42%
are concerned about the lack of transparency in manufacturers' supply chain practices.

Institutions are working with a long tail of vendors, on an average at roughly

- 35–40 third-party platforms per institution.

The supply chain exposure and the higher number of third-party vendors, combined with 7,000-device fleets, explain why many security leaders worry about limited visibility into vendor practices and see secure-by-design, verifiable endpoints as a way to retain trust even when the surrounding edtech ecosystem is hard to control.

From firefighting to foresight: What AI in security should deliver

Leaders who truly understand the risk are turning to AI to counter modern threats, but today's tools still fall short on meaningful, outcome-driven use cases. They want real AI, not buzzwords: When they invest in AI-powered behavioral detection on endpoints, they expect it to catch what signatures miss — advanced phishing and web attacks, cloud and SaaS abuse, fileless and zero-day activity, and misuse of privileged accounts.

"Core AI" feature expectations for modern endpoints



- Correlated telemetry across endpoints
- Automated triage to cut alert fatigue
- Predictive analytics to surface high-risk behaviors
- Automated patching and remediation workflows

"Must-have" AI assist for stretched teams

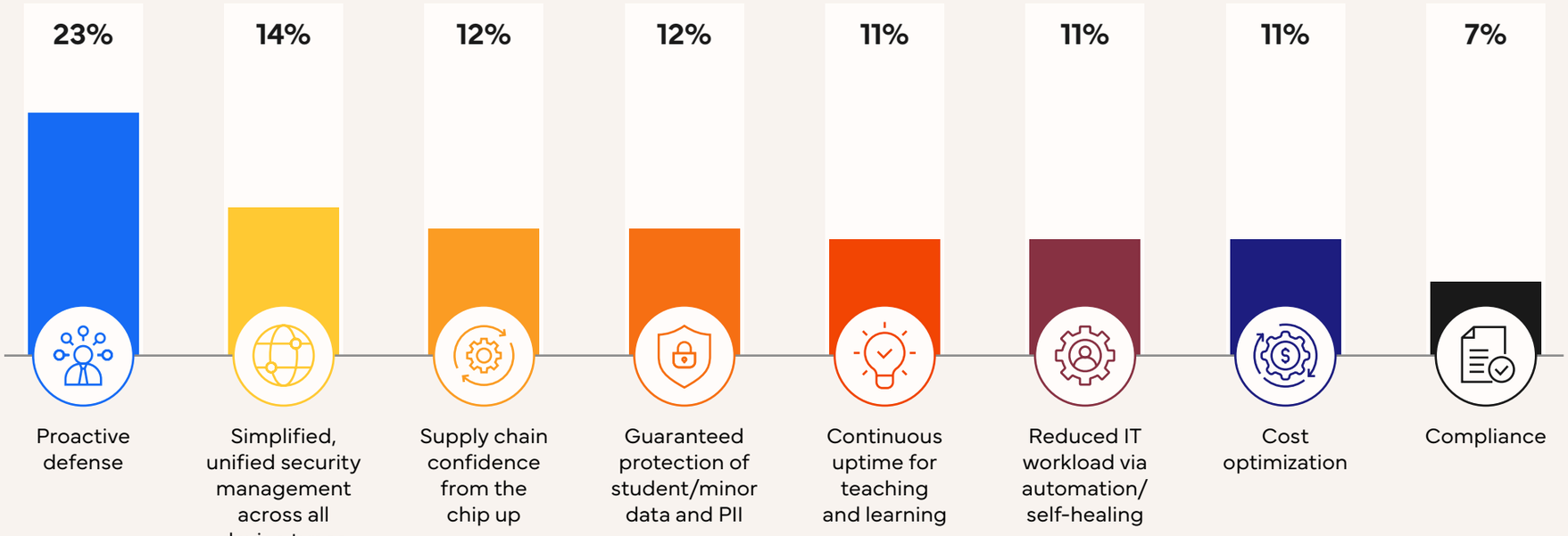


- Take the first pass on detection, triage, and sometimes response.
- Power compliance reporting, device health scoring, and insider behavior analytics.
- Move security from reactive firefighting to a more foresighted, expertise-amplifying posture.

Redefining “good enough” endpoint security

Leaders increasingly recognize that AI-driven security on its own is not enough. Attitudes about where security should live are shifting decisively: Nearly 90% of respondents say protection should be embedded directly into device hardware and firmware by default, reflecting growing skepticism that add-on software can defend low-level components and complex vendor ecosystems.

When they add up these concerns, leaders define a “good enough” security solution as one that should include:



Institutions are frustrated with fragmented tools and worried about whether devices can truly be trusted while treating student safety and instructional continuity as nonnegotiable outcomes, not extras. Taken together, this resets “good enough” endpoint security to mean **proactive chip-to-cloud protection and simplified, unified control that protects students and keeps classes running**.

Why leaders still struggle to change the security model

The survey data shows that the biggest structural barriers for cybersecurity in the education sector are primarily about money, complexity, and organizational priorities:

20%	Cite budget constraints that force trade-offs between basic IT operations and security investment.
18%	Point to the complexity of managing security across diverse device types, campuses, and user populations.
14%	Say cybersecurity is treated as an IT cost center rather than a board-level priority.
12%	Highlight regulatory/compliance burden, and another 11.7% point to cultural resistance from faculty, staff, or students to security measures.
0.2%	Are most concerned about a lack of integrated solutions, with too many disconnected point products.



A security model that fits education, not the other way around

Make endpoint strategy your security strategy. With risk, data, and AI workloads concentrated at the device, choices on architecture, supply chain, and lifecycle are now core security decisions. This directly addresses institutions' top pain point: lack of visibility into device health and posture (36.3%), while also helping enforce more consistent security across owned and BYOD environments (31.1%).

Insist on hardware-anchored security. As attacks drop below the OS and into the supply chain, software-only defenses are no longer enough. Hardware-rooted protection improves trust, strengthens device integrity, and reduces exposure to increasingly sophisticated attacks targeting educational institutions.

Automate or fall behind. At ~7,000 devices per institution and lean teams, self-healing BIOS, automated remediation, and centralized patching are the only scalable path. These capabilities directly reduce alert overload and false positives (34.1%), address the lack of automated remediation (34.8%), and simplify patching for off-network devices (30.4%).

Co-design AI and security. Any device or infrastructure bought for AI learning or research must be judged on how it protects models, data, and access. As institutions expand AI adoption, embedding security into AI initiatives minimizes risk while supporting secure innovation and research continuity.

Use lifecycle and ESG to shrink risk. Secure asset recovery, longer-life and repairable devices, and responsible reuse reduce both emissions and security exposure. Modern lifecycle management also helps institutions deal with aging devices and operational inefficiencies without relying solely on larger budgets.

Technology leaders in the education sector must modernize endpoints and infrastructure with embedded, automated, supply chain–verified security or accept that learning, research, and institutional trust will remain one major incident away from disruption.

About the IDC analyst



Shilpi Handa

Associate Director Research Security and Trust, IDC

Shilpi Handa is an associate research director for IDC's Security and Trust practice, bringing close to 14 years of experience in cybersecurity research and advisory. Shilpi's expertise lies in helping organizations navigate an increasingly complex threat landscape by aligning security strategies with business resilience, innovation, and digital transformation priorities. She has worked extensively across enterprise security architectures, risk management, and operational security, with a strong focus on evolving threat vectors and response capabilities. Shilpi is regularly cited in the media for her insights on cybersecurity trends, AI-driven threats, and the future of digital resilience.

More about Shilpi Handa →

Message from the sponsor

That's the power of Intel Inside®

Intel® trusted supply chain / Intel® hardware-based security / Intel® platforms

Lenovo | intel.

Why lenovo leads in education security:

Lenovo and Intel secure the full attack surface. Securing supply chain, platform, firmware, endpoint, operating system, cloud integration and recovery.

Advanced protection for all

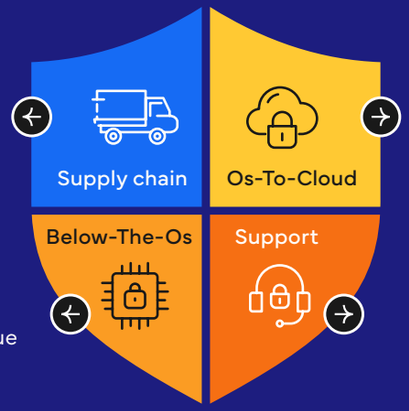
Lenovo ThinkShield delivers comprehensive, modern, and resilient solutions to defend your business.

Secure from the start

End-to-end supply chain protection with verifiable hardware and software assurance.

Security built In, Integrity at every level

Fleet-wide firmware and hardware defense against rogue devices and advanced attacks.



Smarter protection with AI + XDR

AI-powered security that safeguards against ransomware, phishing, and data loss before they happen.

Always On

Expert protection and support, seamlessly handled by one trusted partner, 24x7.

Education outcome: Keep learning and research running securely even when attacks occur

platform foundation with Intel security

- Intel vPro® platform establishes hardware rooted trust at startup
- Intel trusted supply chain supports silicon provenance and platform integrity
- Intel platforms provide secure foundations for AI ready workloads at scale

1. Supply chain assurance:	
Secure from the start	• **Why Education ITDMs care:** Prevent compromised or counterfeit devices from entering the environment. • **Security model:** Supply chain assurance anchored before the device is powered on. • **Lenovo proof:** ThinkShield build assure, powered by Intel trusted supply chain, validates components device integrity and firmware state during manufacturing and delivery, not after deployment.
2. Below the operating system:	
Security built In. Integrity at every layer	• **Why education ITDMs care:** Ransomware and advanced threats increasingly persist below the operating system where EDR has no visibility. • **Security model:** Resilient platform firmware integrity and recovery. • **Lenovo proof:** ThinkShield firmware assurance protects platform firmware integrity, detects unauthorized changes and supports recovery to a trusted state, even if the OS is compromised. Lenovo hardware is secure by design.
3. OS-to-Cloud security:	
Smarter Protection with AI + XDR	• **Why education ITDMs care:** Security teams need correlated signals, not more alerts. Hybrid learning and research environments create visibility gaps once devices leave campus. • **Security model:** Modern OS to cloud detection and response. Comprehensive endpoint security enforced at the device layer. • **Lenovo proof:** ThinkShield XDR, powered by SentinelOne, and Absolute security correlate endpoint threats, device health, persistence and recovery signals, reducing blind spots and response time.
4. Continuous support:	
Always On	• **Why education ITDMs care:** Education IT teams are stretched, and downtime directly disrupts instruction and research. • **Security model:** Resilient lifecycle security with operational support. • **Lenovo proof:** Lenovo security services provide continuous support, including security posture validation, recovery assistance and lifecycle services that accelerate time to trusted state.

IDC Custom Solutions

IDC Custom Solutions produced this publication.
The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA